North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

No federal help for law enforcement. Local and state law enforcement agencies in North Dakota shifted to backup plans April 6, facing the reality that a large portion of the federal aid they had during recent floods likely will not come this year. The only guaranteed assistance with in-the-field emergency operations will be from the U.S. Coast Guard, whose staff and equipment could arrive by April 8, the Cass County sheriff said. Officials with the U.S. Fish & Wildlife Service and Customs and Border Protection said they have had personnel preparing for weeks, but must wait until the U.S. President signs a presidential disaster declaration that the governor of North Dakota requested in February. The President's signature would allow the Federal Emergency Management Agency to dispatch vital federal resources to the Red River Valley. Meanwhile, a government shutdown looms April 8 as Congress attempts to compromise on a budget measure, but officials said federal emergency response resources should not be affected. Source: http://www.inforum.com/event/article/id/315134/

Corps builds clay levees. Contractors hired by the U.S. Corps of Engineers are busy building earthen levees to protect the Fargo-Moorhead and surrounding area from floodwaters. Earth movers are busy building dikes along 2nd Street in Fargo to protect city hall and the high rise and downtown areas from flooding. Wall Street will close in Oakport Township April 5 as the Corps builds an earthen levee across it. River Shore Drive at I-94 in Moorhead was blocked April 5 by a temporary floodwall, and the underpass by the Moorhead Center Mall was closed due to flooding. Source: http://www.kfgo.com/fm-headline-news.php?ID=0000003681

Regional

(Minnesota) **Strong river flow shuts down locks and dams to all traffic in Mpls.** The dangers of the Mississippi River's surging flow have forced the closing April 6 of all three locks and dams in Minneapolis, Minnesota to all traffic well into the middle of the month. The move by the U.S. Army Corps of Engineers comes one day after the locks and dams were closed to just recreational watercraft. The locks and dams affected are the two downtown — the Upper and Lower St. Anthony Falls — and Lock and Dam 1 next to Minnehaha Park. The Corps was required to close the locks and dams because the high flows are unsafe for river navigation at 40,000 cubic feet per second, which is projected to occur April 8. The Corps attributed the strong flow to rain and snow thawing upstream from Minneapolis. Flow estimates from National Weather Service show the possibility of the three locks and dams to remain closed through April 17. Source: http://www.startribune.com/local/minneapolis/119344854.html

(Minnesota) **Recall: Turkey burgers test positive for Salmonella.** Jennie-O Turkey Store of Willmar, Minnesota, recalled nearly 55,000 pounds of frozen, raw turkey burgers because the meat may have been contaminated with Salmonella, federal officials said. Jennie-O said the product was distributed nationwide but sold only at Sam's Club Stores. The U.S. Department of Agriculture's Food Safety and

Inspection Service announced the recall April 2. The USDA could expand the recall as it continues to investigate illnesses connected to products from the Willmar-based turkey processing company, the West Central Tribune reported April 3. So far, 12 people in Arizona, California, Colorado, Georgia, Illinois, Mississippi, Missouri, Ohio, Washington, and Wisconsin have become ill in the last four months. The recall includes 4-pound boxes of Jennie-O's —All Natural Turkey Burgers with seasonings Lean White Meat. Source: http://www.foodmanufacturing.com/scripts/ShowPR~RID~20051.asp

(Montana) **Repairs almost done on dam damaged by bus-sized boulder.** Repairs to the Madison River dam just below Ennis Lake in Ennis, Montana are nearly complete, according to PPL Montana. New gates and the structure supporting them can be seen at the far end of the dam. Last October a bus-sized boulder split off of the nearby cliff and fell on the dam. While the accident did not endanger any people or homes downstream, it caused water levels in Ennis Lake to drop quickly. A PPL spokesman said just removing the huge boulder was a large part of the project. "We drilled holes in the rock and put this pasty grout mixture in these holes and as it dries, it expands and that literally cracks the rock into smaller pieces," the PPL Montana director of external affairs said. Those smaller pieces were then placed in the river downstream of the dam. To make sure more boulders will not fall, PPL drilled holes and installed rods to hold the cliff face steady. The director said there is a good snowpack this year so he expects Ennis Lake to return to normal levels this spring, and for flow on the Madison River to be strong all season. Source: http://www.kpax.com/news/repairs-almost-done-on-dam-damaged-by-bus-sized-boulder/

National

(Louisiana) **Feds: Transocean stonewalling in rig-explosion probe.** The head of the U.S. agency that regulates offshore drilling is questioning Transocean's willingness to cooperate with a key federal investigation of last year's Gulf of Mexico rig explosion and oil spill. The director of the Bureau of Ocean Energy Management Regulation and Enforcement said in a March 31 letter to Transocean that the company has stonewalled on whether it would produce three employees who have been subpoenaed to testify at hearings next week near New Orleans. A lawyer for Transocean, which owned the rig that exploded and which was leasing it to BP, said in a response letter that the company cannot control whether the people that investigators want to question show up or not, but it is willing to produce a different expert who is not on the witness list. The focus of the seventh set of hearings by the U.S. Coast Guard-BOEMRE panel is the blowout preventer that failed to stop the disaster. A report released last week by a firm that tested the device blamed the failure on a faulty design and a bent piece of pipe, appearing to shift some blame for the disaster away from BP and toward Cameron International, which built the blowout preventer, and Transocean, which was responsible for maintaining it. Source: http://www.houmatoday.com/article/20110401/WIRE/110409996/-1/living?Title=Feds-Transocean-stonewalling-in-rig-explosion-probe

International

Floating houses pose bigger test for U.S. Navy, ships than Japan radiation. Houses, cars, and tractor-trailers washed out to sea by the March 11 tsunami are clogging shipping lanes off Japan, posing a bigger challenge to U.S. Navy vessels and commercial lines than radiation from the leaking nuclear plant. The magnitude-9 earthquake that struck off the northeast coast launched a wall of seawater

that obliterated cities and towns, and left more than 27,600 people dead or missing. More than 206,000 buildings were destroyed, damaged or swept away, the Japanese national police agency said April 5. The debris has prompted Japan's coast guard to warn ships to stay about 60 nautical miles away from Tokyo Electric Power Co.'s crippled nuclear-power plant in Fukushima prefecture, north of the capital. That's almost 4 times as far as the 30-kilometer exclusion zone introduced by the government because of concerns about radiation. The U.S. Navy said radiation from the Fukushima Dai-Ichi nuclear plant can be scrubbed off vessels with soap and water. Japan's coast guard posts daily reports about the debris on the Internet, using information gathered from passing vessels. As of April 4, it was recommending that vessels stay up to 90 nautical miles out while passing the zone that suffered the brunt of the destruction from the natural disasters — a 240 nautical-mile stretch from Ibaraki prefecture near Tokyo to Miyagi prefecture in the northeast. Source: http://www.bloomberg.com/news/2011-04-05/floating-houses-pose-bigger-test-for-us-navy-ships-than-japan-radiation.html

Banking and Finance Industry

Chase Bank phish emails may be first post-Epsilon scam. The Better Business Bureau (BBB) warned April 6 that the first post-Epsilon phishing e-mails have been spotted. In this case, cyber-crooks are targeting bank customers with a phony warning and a malicious link. An e-mail purporting to be from Chase Bank that tells users their account will be deleted unless prompt action is taken is currently making the rounds. Users are encouraged to click on the link provided to get to the "profile page" to update their information. JPMorgan Chase was one of the companies affected by the recent Epsilon data breach. Epsilon, a large e-mail marketing services company, disclosed April 1 attackers had stolen customer e-mail addresses belonging to some of its clients. If the "Chase Bank" phish is really related to the Epsilon breach, and not just one of the many fake Chase e-mails seen in the past, it proves the attack on Epsilon was a well-thought-out attack, said the chief technology officer of Application Security. The attackers knew precisely who to go after and what the payoff would be. "Based on the BBB warning, they now appear to be acting very swiftly to carry out their specific phishing attempts," he said. Source: http://www.eweek.com/c/a/Security/Chase-Bank-Phish-Emails-May-Be-First-PostEpsilon-Scam-851226/

SpyEye mobile banking Trojan uses same tactics as ZeuS. Cybercrooks have deployed a sophisticated man-in-the-mobile attack using the SpyEye banking trojan toolkit. The trojan, which infects Windows machines, displays additional content on a targeted European bank's Web page that requests prospective marks to input their cell phone number and the international mobile equipment identity of the device. The bank customer is told the data is needed so a new "digital certificate" can be sent to the phone. The certificate contains the malicious executable (sms(dot)exe) that infects Symbian-based smartphones along with another executable (SmsControl(dot)exe) that displays a message designed to hoodwink users into believing the only thing delivered was a digital certificate. Net security firm F-Secure detects this malware as Spitmo-A. The European bank targeted in the attack uses short message service (SMS)-based mobile transaction authentication numbers (mTANs) to authorize transfers. Details of how the SMS-based mTANs are delivered to the attacker are still under investigation, but preliminary research suggests they are delivered via hypertext transfer protocol, and not via SMS as with an otherwise similar earlier attack that used the infamous ZeuS cybercrime toolkit. The earlier ZeuS-based attack also used a file called SmsControl(dot)exe as part of its payload. Presenting a trojan as a digital certificate, one of the tricks of the SpyEye-based attack, also appeared

in the earlier ZeuSMitmo attack. Despite these similarities, and the rumored merger between ZeuS and SpyEye, the two strains of malware are otherwise dissimilar, F-Secure reports. Source: http://www.theregister.co.uk/2011/04/05/spyeye_mobile_trojan/

Identity theft criminals may target U.S. children more than adults, new report suggests. AllClear ID announced April 1 the release of the first large child identity theft report ever published; based on identity protection scans of more than 42,000 U.S. children, it suggests a previously unrecognized demographic for what the FBI has named the fastest growing crime in the United States. Authored by a distinguished fellow at Carnegie Mellon CyLab, the report revealed that 10.2 percent of the child identities scanned (4,311 victims) had someone else using their Social Security number — 51 times more frequently than the 0.2 percent rate for adults in the same population. The report shows stolen Social Security numbers for children as young as 5 months old are being used to secure employment, open credit card and bank accounts, purchase homes and automobiles, and obtain driver's licenses. As a result of this new cyber epidemic, children are discovering their credit and credibility are destroyed just as they enter adulthood. As a consequence, they are being denied internships, student loans, and apartments due to attacks on their identity that occurred years earlier. Experts predict the damage to children will get even worse with health-care identity theft on the rise. The report offers an analysis of over 42,000 identity protection scans performed on U.S. children (age 18 and under) during 2009-2010. The research was conducted using a patented technology called AllClear ID. Source: http://uspolitics.einnews.com/pr-news/368686-identity-theft-criminals-may-target-u-s-children-more-than-adults-new-report-suggests-

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

Nothing Significant to Report

Communications Sector

Verizon customers exposed in massive epsilon data breach. Customers of Verizon Communications had their e-mail addresses exposed in a massive online data breach the week of March 28, according to an e-mail to customers obtained by Reuters. In what could be one of the biggest such attacks in U.S. history, a computer hacker penetrated the online marketer Epsilon, which controls the customer e-mail databases for a broad swath of companies. Customers of about 50 companies, from banks to retailers and hotels, had their names or e-mail addresses exposed in the attack. Verizon, the largest U.S. mobile phone carrier, informed customers April 5 that it was part of the Epsilon data breach. "Epsilon has assured us that the information exposed was limited to email addresses, and that no other information about you or your account was exposed," Verizon said in an e-mail to a customer sent April 5. Source: http://www.huffingtonpost.com/2011/04/06/verizon-epsilon-data-breach_n_845379.html

Rep. Giffords inspires mobile communications legislation. ABC News reports that a U.S. Representative from Texas introduced legislation March 31 to improve cellular service near the U.S.-Mexico border at the request of an Arizona Representative. The Arizona Representative was preparing to introduce the legislation at the start of the 112th Congress before she was shot January 8 in Tucson, Arizona. The legislation, called the —Southern Borderlands Public Safety Communications Act, would authorize grant funding through the Department of Homeland Security for public-private partnerships to better develop mobile communications near the border. The Texas Representative told ABC News that the senator was inspired to introduce the legislation after one of her constituents was murdered by Mexican drug smugglers who came onto his property after he was unable to get cell phone service and call 911. The President has also sought to improve mobile communications by calling for a National Wireless Initiative that aims to provide 98 percent of Americans with access to high-speed internet. Source: http://www.nextgov.com/nextgov/ng_20110401_2411.php?oref=topnews

Critical Manufacturing

Saab halts plants again. Saab Automobile, the Swedish carmaker owned by Spyker Cars NV, halted production April 6 as renewed disputes with suppliers strangled delivery of components for the second time in 8 days. "We're starting to get really worried," the chairman of Swedish automotive supplier group FKG, said in a telephone interview. "You can't have it this way, stop-and-go, stop-and-go. It isn't making anybody happy." Saab is in discussions with some suppliers about payment and delivery terms, a spokeswoman said, adding she was not sure when production would resume. Saab halted production March 29 after some suppliers withheld materials deliveries over late payments. Spyker's chief executive officer told reporters April 5 the supplier issue was under control. "We're discussing very intensively with our suppliers to reach an agreement in order to restart the flow of material," she said April 6. She declined to identify the suppliers or to say how many there are. Saab's chief executive officer said April 6 the Trollhaettan, Sweden-based company's liquidity "became more strained" during the second half of the first quarter, declining to give more details. Saab sold 31,696 cars in 2010, below a forecast it had in September of 45,000 cars. It later lowered the forecast to between 30,000 and 35,000 cars. Source: http://www.detnews.com/article/20110407/AUTO01/104070353/1148/auto01/Saab-halts-plants-again

Toyota says most Japan plants to stay idle next week. Toyota Motor Corp said April 6 it would not restart production at most of its idled Japanese vehicle assembly factories the week of April 11, denying a Nikkei newspaper report. The world's biggest automaker has halted vehicle assembly at all but 2 of the 18 group-wide factories in Japan that build Toyota and Lexus cars since the March 11 earthquake and tsunami disrupted supply of components to automakers globally. "There will be no resumption of production at most of our domestic factories next week [the week of April 10]," a Toyota spokeswoman said. The company will announce its decisions as they are made, she said. Japan's Nikkei business daily reported Toyota would reopen most of its domestic automobile plants as early as the week of April 10 to start producing a limited number of models. Toyota had lost potential production of about 200,000 vehicles as of April 1, it said, with April 6 marking the 18th day of suspension at most of its Japanese factories. Among other major Japanese automakers, Honda Motor Co. has said it aims to restart production at all domestic plants April 11 at a rate of about half its original plans. Nissan Motor Co. plans to resume normal production with parts procured from

suppliers, rather than using inventory, from mid-April at limited operation levels. Source: http://www.reuters.com/article/2011/04/06/us-toyota-idUSTRE7350DL20110406

Ford to idle plants, Nissan adjusts output schedule. Ford Motor Co will idle its Kentucky pick-up truck plant the week of April 3 and Nissan Motor Co Ltd will adjust its production schedule due to parts shortages caused by the earthquake in Japan 3 weeks ago. The Louisville, Kentucky, plant is the first U.S. plant that Ford is shutting because of supply chain issues related to plant closings in Japan. Ford declined to say which parts or suppliers were involved when it announced the move April 1. Ford also said it would idle two other plants the week of April 3 in Michigan and Mexico, but the automaker said it was not for issues related to the Japan crisis. Ford builds its —Super Duty heavy trucks at the plant in Louisville, as well as the Ford Expedition and the Lincoln Navigator. Additionally, Nissan said it would adjust the output schedule at auto plants in the United States and Mexico by shifting non-production days planned for later in the second and third quarters to April. All three of Nissan's plants in the United States will be idled April 8 and April 11 as well as April 18 through April 21. Nissan will also shut down its plant in Cuernavaca, Mexico, the week of April 3 and another plant in Aguascalientes the week of April 10. Nissan said the changes were made to avoid major supply disruptions and because some parts shipments are still in transit from Japan. Source: http://www.reuters.com/article/2011/04/01/japan-usa-autoplants-idUSN0128180020110401

Defense/ Industry Base Sector

Law firms under siege. Law firms are increasingly getting hit by stealthy, low-profile targeted attacks going after intelligence on their corporate clients, Darkreading reported April 6. Forensics investigators at Mandiant are working on twice as many targeted attacks by so-called advanced persistent threat (APT) adversaries against law firms than in years past; of the commercial victims Mandiant investigated during the past 18 months or so, 10 percent were law firms. And those are only the cases Mandiant sees: Its executives said many more go unnoticed by the victim organizations. Law firms are joining the ranks of federal government agencies, defense contractors, and technology companies (like Google and RSA) as targets for APTs because "[l]aw firms are a means to an end: a defense contractor or utility" that they represent, for example, said the vice president of professional services at Mandiant. He said while he worked on just a handful of cases where law firms were hit, he now sees a dozen to 15 at once. Attackers find law firms an attractive and relatively soft target for gathering the intelligence they want on a new weapons system or software, for example. Firms that represent clients in mergers and acquisitions, or civil litigation, are getting hit, including when their clients are involved with deals involving Chinese companies. Source: http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/229401089/law-firms-under-siege.html

Emergency Services

(California) **Calif. officers call new law a 'disaster'.** AB109 was signed into law April 4 in California. The law releases thousands of prisoners to jails, leaving local law enforcement responsible for low-level offenders convicted of nonserious, nonviolent, and nonsexual offenses. Some law enforcement organizations called on the governor to delay signing the bill until the money is in place to pay for more jails, rehabilitation programs, and alternative sentencing, such as house arrest. Law

enforcement organizations want a guarantee built into the state constitution to make sure they still get the funds once the governor leaves office. The law affects only offenders convicted after July 1, with current inmates remaining under the state's supervision. Source: http://officer.com/online/article.jsp?siteSection=1&id=57721

Obama signs policy directive on government's emergency preparedness. The U.S. President signed a national-security directive the week of March 28 designed to put the administration's imprint on the way the nation responds to major emergencies, including terrorism, National Journal reported. A senior administration official said that congressional committees were briefed April 5 on the Presidential Policy Directive, which bears the title of "National Preparedness." The directive sets government policy as informed by a National Security Staff review completed earlier this year. According to a summary of the directive given to National Journal, the administration preserves core elements of the former U.S. President administration's emergency preparedness plan, which was released in 2003. It makes DHS grants contingent on performance and on how the Homeland Security Secretary assesses need and the quality of response plans. The directive also instructs DHS to set up a "National Preparedness System," which the summary said "will enable the nation to achieve the goal" of maximum preparedness and to undertake "a comprehensive campaign to build and sustain national preparedness; and an annual National Preparedness Report to measure progress in meeting the goal." The directive also calls for closer collaboration with the private sector, and for better and more effective ways for the government to communicate with communities during crises. Source: http://www.govexec.com/dailyfed/0411/040611emergency-response.htm

NORTHCOM striking military emergency response deal with governors. The Department of Defense (DoD) is negotiating with state governors to set rules for more extensive use of the U..S military during a national disaster, including the activation of Army Reserves, the commander of U.S. Northern Command (NORTHCOM) revealed April 5. DoD has the authority to activate Reserves on an involuntary basis, the U.S. Navy Admiral and NORTHCOM commander said during a hearing of the Senate Armed Services Committee, but state governors have resisted the notion in the past as they like to maintain control of armed forces operating within their states during a disaster. NORTHCOM has been engaging U.S. governors to gain their approval for use of the dual-status structure, which would include a deputy commander acting in federal status, as well as the activation of Reserve forces. The deputy commander, acting under U.S. Code Title 10, would be able to bring federal resources directly to bear against a disaster scenario, an official noted. NORTHCOM also is working with the National Guard to improve its readiness for chemical and biological threat response as well as border security. Source: http://www.hstoday.us/industry-news/general/single-article/northcom-striking-military-emergency-response-deal-with-governors/4528e3e0e5d9138c438f89f3e3827ebc.html

Energy

U.S. pushes crackdown on gas, oil pipeline owners, operators. A series of pipeline incidents, including one in 2010 near Marshall, Michigan, prompted the U.S. Transportation Secretary April 4 to call for pipeline owners and operators to conduct a comprehensive review of their lines, and accelerate critical repair and replacement work. The Transportation Secretary is pushing for

legislation to increase the maximum penalty for pipeline violations from $100,000 per day to $250,000 per day, and from $1 million for a series of violations to $2.5 million. In a news release April 4, he urged Congress to give his department — which oversees pipeline safety and enforcement — authority to close regulatory loopholes, add inspectors, and strengthen requirements for risk management, safety, and data reporting. A pipeline safety forum is planned for April 18 in Washington D.C. to discuss what improvements are needed for the nation's pipeline infrastructure. Source: http://www.freep.com/article/20110405/NEWS15/104050331/U-S-pushes-crackdown-gas-oil-pipeline-owners-operators

Energy infrastructure lacks advanced defense from cyber attacks. A majority of energy and utility companies do not use "state-of-the art" technology to defend their networks and are exposing critical infrastructure to sophisticated cyber attacks, a new industry survey said. Sixty-seven percent of information technology professionals surveyed said their organizations had not deployed the best available security to guard against hackers and Internet viruses, states a report released April 6 by Ponemon Institute LLC, an information-security research group. Of the 291 security practitioners who responded, 71 percent said their companies' top executives do not understand or appreciate the value of information-technology security, according to the report. "One of the big surprises in this survey was that despite increasing cyber attacks on networks, the strategic importance of IT security among C-level executives hasn't increased," said the senior vice president of marketing and channels for Q1 Labs Inc., a software company that sponsored the survey. "It seems that the industry is very reactive in terms of IT security investment." The report follows recent high-profile cyber attacks, including the Stuxnet computer worm, which affects machines sold by Munich-based Siemens AG and can take over networks that run factories and power plants. The Ponemon report also identified shortcomings in adhering to industrywide regulatory initiatives. Seventy-seven percent of survey respondents said compliance with industry security standards did not rank as a priority at their organizations. U.S. regulators currently lack the authority to issue and enforce rules for protecting electric grids from cyberthreats, leaving the industry to follow its own voluntary standards. Those guidelines are set by the North American Electric Reliability Corp., an industry self-regulatory group that helps companies assess their ability to respond to potential attacks. Source: http://www.bloomberg.com/news/2011-04-06/energy-infrastructure-lacks-advanced-defense-from-cyber-attacks.html

Food and Agriculture

(Louisiana) **Lethal Listeria outbreak tied to hog head cheese.** In August, 2010, a half million pounds of sausages and hog head cheese were pulled off Louisiana grocery shelves in a recall triggered by what the state department of agriculture and forestry said were Listeria monocytogenes isolates detected in a product sample from Veron Foods. The contamination was discovered in the Prairieville-based company's products, according to the news release, "through a foodborne illness investigation." There was no indication of whether that meant one illness or multiple illnesses. Less widely circulated than the recall notice, however, was the Louisiana Morbidity Report, September-October 2010, which on page 5 revealed that behind the recall was a significant foodborne illness outbreak — 14 cases of listeriosis. The Louisiana Listeria outbreak is now disclosed in detail by the U.S. Centers for Disease Control and Prevention (CDC) in its most recent Morbidity and Mortality Weekly Report, issued April 7. CDC said the case was the first published report of an invasive

listeriosis outbreak associated with hog head cheese. The CDC report also mentions something else the Louisiana report did not: seven of the 14 listeriosis cases were so severe the individuals had to be hospitalized. And two of the case patients died. Source: http://www.foodsafetynews.com/2011/04/first-invasive-listeriosis-linked-to-hog-head-cheese/

Radioactive materials found in fishnear stricken Japan nuclear plant. Japanese authorities reported April 5 they hadfound unusually high levels of radioactive materials in fish caught about 80 kilomefrom a stricken nuclear plant, stoking concerns radioactive water from the plant threatens marine life, and possibly a key food source for the country. According to Ibaraki prefectural government, two samples of small fish called konago, or young lance fish, caught at separate locations near the Pacific coast of northern Ibaraki hahigher-than-permissible levels of radioactive materials. In one sample collected Ap**ne** uine er 18 the t the d ted wo d at ce ning als meat he mes. ng ters the d ril 1, a local fishery cooperative detected 4,080 becquerels per kilogram of radioactive iodine. While Japan had not set a limit for acceptable iodine levels in seafood, the government April 5 set the limit at 2,000 becquerels per kilogram, the same as for vegetables. In another sample collected April 4, 526 becquerels per kilogram of cesium was detected in fish, exceeding the 500-becquerel limit. The findings were the first clear indication of radioactive contamination in fish following leakage of radioactive water from Fukushima Daiichi nuclear plant, which was battered by the March 11 earthquake and tsunami. The discovery of contamination in fish will likely add to fears the release of radioactive water from the plant will lead to widespread contamination. The plant's operator, Tokyo Electric Power Co., dumped 3 million gallons of low-level radioactive water into the Pacific Ocean April 4 in an effort to avoid the release of even more highly contaminated water from the plant. Source: http://online.wsj.com/article/SB10001424052748703712504576244251331137870.html

Drug-resistant Salmonella linked to turkey recall. The Salmonella strain that sickened 12 people in 10 states and triggered the April 1 recall of 54,960 pounds of Jennie-O turkey burgers may be resistant to antibiotics, the Centers of Disease Control and Prevention (CDC) announced April 4. According to CDC, Salmonella Hadar is resistant to many commonly prescribed antibiotics, including ampicillin, amoxicillin/clavulanate, cephalothin, and tetracycline, which may increase the risk of hospitalization or possible treatment failure in infected individuals. Jennie-O Turkey Store recalled 4-pound boxes of frozen Jennie-O Turkey Store "All Natural Turkey Burgers with seasonings Lean White Meat" containing 12 individually wrapped one-third pound burgers after they were linked to 12 confirmed cases of Salmonella Hadar in Arizona, California, Colorado, Georgia, Illinois, Mississippi, Missouri, Ohio, Washington, and Wisconsin, with illnesses occurring between December 2010 and March 2011. Three of the patients in Colorado, Ohio, and Wisconsin specifically reported eating this product prior to illness onset and hospitalization; the last of these illnesses was reported March 14. Source: http://www.foodproductdesign.com/news/2011/04/antibiotic-resistant-salmonella-linked-to-turkey.aspx

USDA: Delay in meat sales could prevent recalls. The U.S. President's administration is aiming to prevent meat recalls by withholding meat and poultry products from grocery store shelves until government testing is complete. The Agriculture Department proposed rules April 5 that would force companies to delay shipments to consumers until government inspectors have released tests on the meat. The department's Food Safety and Inspection Service has inspectors in all meat plants that sample for E. coli and other contaminants. Currently, products that are sampled can be shipped

before testing results are known, though many companies already have procedures in place to hold the meat. The agency said at least 44 recalls between 2007 and 2009 could have been prevented if the rule had been in place. Source: http://www.whec.com/news/stories/S2051669.shtml?cat=566

Government Sector (including Schools and Universities)

Profile Spy scam hits Twitter. Security researchers warn of a survey scam currently making the rounds on Twitter which tricks users by promising them the ability to view their profile visitors. According to a researcher from Errata Security, victims post spam messages that read "94 people viewed my profile today!" followed by "Wow! See who viewed your twitter with Profile Spy [link]" Clicking on the link takes users to a page asking for an app called "Profile Spy" to connect to their accounts. This app is used for the scam's propagation and if allowed, it will start sending spam from the victim's accounts without their permission. People who agree to connect with the application will be redirected to a page asking them to participate in a survey, allegedly as a security check. These surveys try to sign up users for premium rate mobile services or are part of legit affiliate marketing campaigns that are abused by the scammers. Each time a user completes a survey, the scammers earn a commission, which makes it worthwhile to keep the attacks going. "There might be further malware in those links designed to compromise your machine or accounts, like clickjacking exploits," the researcher warned. Source: http://news.softpedia.com/news/Profile-Spy-Scam-Floods-Twitter-193106.shtml

(Kentucky) **Kentucky releases homeland security terrorist reporting app.** Kentucky's Office of Homeland Security (KOHS) released an iPhone app designed to allow people to anonymously report any suspicious activity. The app, called, Eyes and Ears on Kentucky, captures tips in real-time and is capable of providing additional information using the iPhone's camera and Global Positioning System features. The app is part of the broader national DHS "See Something Say Something" campaign to gather tips from across the nation and allow local, state, and federal law enforcement officials to sift through reports of any suspicious activity. KOHS is encouraging citizens to report people engaging in any suspicious activity, including people taking photos or videos of buildings, asking detailed questions about public transportation, and loitering near critical infrastructure. The app was developed in conjunction with state employees who helped build the Kentucky.gov Web site. Source: http://homelandsecuritynewswire.com/kentucky-releases-homeland-security-terrorist-reporting-app

Safeguarding the private and public sector from insider threats. A recent panel at the Government Security Convention and Expo in Washington, D.C. dealt with the full range of threats posed by insiders. These types of threats are often the most difficult to detect as they originate from individuals who have already been screened and given access to an organization's critical resources. Businesses, government agencies, and other organizations are vulnerable to a host of threats from insiders including corporate espionage, workplace violence, and the loss of data. Speaking on the panel, the deputy general counsel to the U.S. Senate Homeland Security Committee described the legislative push to secure federal facilities. Currently, the Federal Protective Service (FPS) is charged with overseeing security at 9,000 federal facilities across the nation, but the organization has proven unable to effectively protect employees and prevent illegal materials from being smuggled into buildings. According to the deputy general counsel, Government Accountability Office (GAO) reports

and independent investigations by the DHS Inspector General "have documented serious and systematic flaws within the operations of FPS." "These lapses place federal employees and private citizens at risk every day," she said. As evidence, she cited an undercover investigation by GAO in June 2009, where investigators successfully smuggled bomb-making materials into 10 federal facilities and were not detected, even as they assembled the parts. Source: http://homelandsecuritynewswire.com/safeguarding-private-and-public-sector-insider-threats?page=0,0

(New York) **Terror threats made against Long Island school buses.** An anonymous but threatening e-mail was sent April 1 to various New York State offices and state officials, including the speaker of the house. The e-mail referenced threats of violence in state office buildings, against the state legislature, and also made a specific reference to school buses. Because of this, the New York State Education Department issued an e-mail to schools April 4, urging school bus drivers and dispatchers to take extra precautions in checking buses and making sure students are safe. School bus drivers and dispatchers said they had read the e-mail, and that they already receive regular counterterrorism and safety training at the start of each year. New York State Police, the state office of counterterrorism, and the FBI are investigating. The state department of education encourage people involved in school bus transport to remain aware of their surroundings and report suspicious activity. Source: http://www.wpix.com/wpix-li-bus-threat,0,5006745.story

(New York) **Email threat sent to state lawmakers.** New York State Police are investigating a threatening email sent to all New York state legislators early April 1. The 458-word message from someone claiming to be a state employee was titled —Time to Kill. —News reporters, politicians, and the wealthy are all going to be targets, the message said. —I personally am going to use my position and contacts in state government to gather information about the vulnerabilities of public and private targets in New York, the writer said in the e-mail. —Understand with whom you are dealing. I am not crazy. I am a terrorist. I stand for all of the people who don't have a voice, the sender wrote. The writer claimed he or she talked to a state legislator about three years ago. —Both the Speaker and the Senate Majority Leader, and the Governor are taking it seriously, a state Senator said. Source: http://www.democratandchronicle.com/article/20110403/NEWS01/104030361/0/NEWS0201/Email-threat-sent-state-lawmakers?odyssey=nav|head

Information Technology and Telecommunications

EFF reveals more bad digital certificate signing practices. The Electronic Frontier Foundation (EFF) warned that certification authorities (CAs) have signed tens of thousands of digital certificates for unqualified names, some of which even passed extended validation. The EFF, one of the leading digital rights watchdogs, reached this conclusion after analyzing data from its SSL Observatory project that looks for weaknesses in the public key infrastructure (PKI). Digital certificates are used to establish encrypted connections and trust on the Internet, which makes them a vital part of security. The EFF warned that aside from hardcoding usernames and passwords in tools used by resellers and failing to perform proper checks for certificate requests received from them, CAs also sign unqualified names. In practice, there should be a single certificate per domain or subdomain. However, it turns

out some CAs have signed certificates for names like “exchange”, “mail” or “wiki,” which cannot be accessed over the Internet and are sometimes used on local networks. Another name for which there are thousands of valid certificates in existence is “exchange” and variations of it, like “exchange01”, “exchange02” etc. But not only have CAs signed certificates for unqualified names, many of them signed multiple ones for the same host. In total, the EFF has counted 37,244 valid certificates that should not exist. A separate investigation performed in January uncovered 10 EV certificates of the same type. This represents a very serious abuse of trust, because EV stands for extended validation and these certificates are supposed to be issued after extensive identity checks. The main concern is that if any of these certs falls in the hands of attackers, they can be used to impersonate mail and other types of servers on networks that use those names internally. Source: http://news.softpedia.com/news/EFF-Reveals-More-Bad-Digital-Certificate-Signing-Practices-193678.shtml

Popular open source DHCP program open to hack attacks. The makers of the Internet’s most popular open source DHCP program April 5 warned that it is vulnerable to hacks that allow attackers to remotely execute malicious code on underlying machines. The flaw, which is present in Internet Systems Consortium’s (ISC) dynamic host configuration protocol (DHCP) versions prior to 3.1-ESV-R1, 4.1-ESV-R2, and 4.2.1-P1, stems from the program’s failure to block commands that contain certain meta-characters. The vulnerability makes it possible for rogue servers on a targeted network to remotely execute malicious code on the client, ISC warned. ISC advises users to upgrade. Users can in some cases follow workarounds, which include disabling hostname updates or configuring their systems to access only legitimate DHCP servers in settings where access control lists are in place. DHCP is a system for automatically assigning computers IP addresses on a given network and helping administrators to keep track of those assignments. ISC said its DHCP program is the most widely used open source DHCP implementation on the Internet. Source: http://www.theregister.co.uk/2011/04/07/dhcp_remote_vuln/

Xbox LIVE policy director has online accounts hijacked. A disgruntled gamer has managed to hijack the domain, e-mail, and Xbox accounts of Microsoft’s director of policy and enforcement for Xbox LIVE. It appears the hack began with a social engineering attack against Network Solution, the registrar used by the policy director for his stepto.com domain. With control over the domain, the hacker managed to obtain access to the director’s personal @stepto.com e-mail address and used it to reset the password for his Xbox LIVE account. The attacker, who calls himself Predator, posted a video of him controlling the account on YouTube. Apparently, he was annoyed with the director for repeatedly banning him. As director of policy and enforcement for Xbox LIVE, the victim is responsible for banning people who try to cheat the system. The hacker also offered to hijack other people’s accounts for a price of $250. Source: http://news.softpedia.com/news/Xbox-LIVE-Policy-Directors-Has-Domain-and-Online-Accounts-Hijacked-193068.shtml

Attack hijacks sensitive data using newer Windows features. Security researchers have outlined a way to hijack huge amounts of confidential network traffic by exploiting default behavior in Microsoft’s Windows operating system. The man-in-the-middle attacks described April 4 take advantage of features added to recent versions of Windows that make it easy for computers to connect to networks using the next generation IPv6 protocol. The attack will also work against Apple’s OS X for Macs, although the proof-of-concept has not been tested on that platform, said a

program manager at InfoSec Institute, an information security services company. The attack exploits an industry standard known as Stateless Address Auto Configuration (SLAAC) for allowing clients and hosts to find each other on IPv6 networks. When the next-generation addressing scheme is turned on, as it is by default in OS X, Windows Vista, Windows 7, and Server 2008, SLAAC can be used to create an unauthorized IPv6 network that reroutes data through hardware controlled by the attackers. "All these Windows boxes will default connect to the evil router instead of the legitimate router when this parasitic overlay is running," the researcher told The Register. "If Microsoft didn't have that configuration by default, it would negate a lot of the effects of the attack." Source: http://www.theregister.co.uk/2011/04/04/slaac_attack_microsoft_windows/

About 50 clients hit by Epsilon e-mail marketing breach. About 50 companies were affected by a major security breach at e-mail service provider Epsilon Interactive that caused many U.S. corporations to warn their customers of online attacks April 4. Epsilon first warned of the incident April 1, saying that someone infiltrated company systems and obtained e-mail addresses and names belonging to some of its customers. However, it was not immediately clear how many of its 2,500 clients were at risk. Epsilon still has not disclosed much information about the problem, but it has now given a clearer picture of how many companies are affected. In a brief statement posted to Epsilon's Web site April 4, the company said that "approximately 2 percent of total clients" — about 50 businesses — were hit. Customers of many of these businesses received e-mail warnings April 4, telling them that their e-mail addresses had been stolen, and that spam or malicious messages could be coming their way. So far, Epsilon has refused to provide a detailed list of all companies that were affected. Companies hire Epsilon to send out a total of more than 40 billion messages on their behalf each year. With millions of addresses thought to have been stolen, the problem may be worse than many people realize, security experts said April 4, because once scammers know their victims' names and e-mail addresses, along with the companies that they do business with, they can craft very targeted "spear-phishing" e-mail attacks that try to trick victims into revealing more sensitive information such as passwords or account numbers. Source: http://www.computerworld.com/s/article/9215488/About_50_clients_hit_by_Epsilon_e_mail_marketing_breach

DHCP client allows shell command injection. The Internet System Consortium's (ISC) open source DHCP client (dhclient) allows DHCP servers to inject commands that could allow an attacker to obtain root privileges, according to a new ISC advisory. The problem is caused by incorrect filtering of metadata in server response fields. By using crafted host names, and depending on the operating system and what further processing is performed by dhclient-script, it can allow commands to be passed to the shell and executed. A successful attack does, however, require there to be an unauthorised or compromised DHCP server on the local network. Dhclient versions 3.0.x to 4.2.x are affected. The ISC has released an update. Source: http://www.h-online.com/security/news/item/DHCP-client-allows-shell-command-injection-1222805.html

ZeuS source code availability worries researchers. Security researchers worry that ZeuS source code, which is already available for sale on the underground market, could become widely available for anyone to use. In 2010, Slavik, the author of ZeuS left the trojan's code base to the creator of the competing SpyEye crimeware, Gribodemon. His intention was for his rival to offer support to existent ZeuS customers and combine the two threats into one super trojan that had the best features of

both. However, sometime afterwards someone put the ZeuS source code up for sale, making it clear that there is more than one copy of it. According to researchers from antivirus vendor Trend Micro, Gribodemon posted a message claiming that Slavik also sold the source code to someone else for $15,000. It is possible the person is now trying to resell it to others for a profit. —We are predicting that soon the source code will be in the hands of anyone that wants it, the Trend experts say. —This could be potentially dangerous, but only if it gets into the hands of people who really know how to use it, they add. Apparently the ZeuS code is filled with macros that link different parts together. Pulling out individual components for reuse in another malware is not something that just any programmer can accomplish. Source: http://news.softpedia.com/news/ZeuS-Source-Code-Availability-Worries-Researchers-192775.shtml

Photoshopped image scam used in rogue Facebook app trap. Facebook users were put under fire April 4 by a brace of new threats, one of which spreads through a link disseminated through the Facebook Chat application. An estimated 600,000 people have already clicked onto the link, which falsely promises to show them a funny Photoshopped image of themselves. In reality, users install a rogue application which sends messages to their contacts via the social network's instant messaging feature, thus continuing the infection cycle. Users are taken to a fixed gallery of 45 photoshopped images, none of which feature the person who followed the link. M86 Security reports that the scam, whose purpose is unknown, is spreading quickly, attracting new victims at the rate of around 90,000 clicks per hour. Presently, no malware is being spread through the ruse. Source: http://www.theregister.co.uk/2011/04/04/photoshop_image_facebook_scam/

More customers exposed as big data breach grows. The names and e-mails of customers of Citigroup Inc and other large U.S. companies, as well as College Board students, were exposed in a massive and growing data breach after a computer hacker penetrated online marketer Epsilon. In what could be one of the biggest such breaches in U.S. history, a diverse number of of companies that did business with Epsilon stepped forward over the weekend of April 3 to warn customers some of their electronic information could have been exposed. Drugstore Walgreen, Video recorder TiVo Inc, credit card lender Capital One Financial Corp, and teleshopping company HSN Inc all added their names to a list of targets that also includes some of the nation's largest banks. The names and electronic contacts of some students affiliated with the U.S.-based College Board — which represents some 5,900 colleges, universities and schools — were also potentially compromised. No personal financial information such as credit cards or social security numbers appeared to be exposed, according to the company statements and e-mails to customers. Epsilon, an online marketing unit of Alliance Data Systems Corp, said April 1 that a person outside the company hacked into some of its clients' customer files. The vendor sends more than 40 billion e-mail ads and offers annually, usually to people who register for a company's Web site or who give their e-mail addresses while shopping. Law enforcement authorities are investigating the breach, though it was unclear April 3 how many customers or students had been exposed. Epsilon is also looking into what went wrong. Source: http://www.foxbusiness.com/technology/2011/04/04/customers-exposed-big-data-breach-grows/?test=latestnews

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

(Florida; Michigan; Minnesota; Texas) **Health officials dealing with measles outbreak.** The Orange County Health Department in Florida reported that three tourists from Minnesota, Michigan, and Texas came down with measles after they visited Orlando in March. In Minnesota alone, WFTV found out, there are as many as 15 cases of measles and they are the first cases to surface in years. Health officials said they have no idea how the outbreak started, other than that the infected individuals came through Orange County. They do not know if they made contact with someone who lives in the county and had the measles, or were infected by another traveler moving through Orange County. There have been no reported cases of measles in Orange County, and because the incubation rate of measles is 8 to 12 days and health officials said, so far, it does not appear that the infected were also spreading the virus while they were in Orlando. Source: http://www.wftv.com/news/27451133/detail.html

(Virginia) **Whooping cough outbreak in Floyd County blamed on lax vaccinations.** A small, private Floyd County, Virginia school has closed for the week after more than half its students became ill with whooping cough. At least 30 people associated with Blue Mountain School have been diagnosed with the highly contagious disease, also called pertussis, including 23 of its 45 students, said the alternative school's director. The Virginia Department of Health is working with the school to contain the outbreak. While the majority of the cases involve children, a few adult cases have been identified, the director of the New River Health District said. The outbreak was caused by not properly vaccinating people against the disease, she said, noting that a subset of the population does not follow vaccination recommendations. Source: http://www.roanoke.com/news/roanoke/wb/282419

Data breach mistakes feared more than hackers by compliance professionals. Seventy percent of compliance professionals feel their organizations are well or very well prepared to fend off hacker attacks, however, their confidence wanes significantly when assessing other data breach threats, according to a survey conducted by the Society of Corporate Compliance and Ethics (SCCE) and the Health Care Compliance Association (HCCA). Fully 61 percent believed an accidental breach by an employee was very or somewhat likely, and 41 percent felt the same way about accidental breaches by third-party vendors. "The fear over unintentional breaches suggest that employees and vendors still don't fully understand the need to safeguard data and despite training, people will still make mistakes," said the SCCE and HCCA chief executive officer. The survey found 82 percent of those responding had invested more time on the issue of data privacy compliance in the previous year. This

investment is expected to continue with 77 percent of respondents indicating they expect time spent on data protection and privacy to further increase during the next year.Source: http://www.prnewswire.com/news-releases/data-breach-mistakes-feared-more-than-hackers-by-compliance-professionals-119183644.html

(Hawaii) **Four confirmed dengue fever cases, 12 more suspected.** State health officials say two suspected cases of dengue fever have been confirmed, bringing the total to four in the Pearl City, Hawaii area. But there are 12 more suspected cases in different parts of Oahu. The State Department of Health received 20 reports of possible dengue fever from physicians since issuing its medical alert the week of March 28. Eight were quickly ruled out but 12 cases are pending. Results of those blood tests are expected the week of April 4. A doctor with the CDC's dengue branch said the carrier of dengue in Hawaii is the Asian Tiger mosquito. —The only way these Asian Tiger mosquitoes get it or these Aedus Albopitus for the scientific name mosquitoes get it is that they have to bite somebody with dengue, so humans are actually the source of their infection, he said. He added most infected people show no symptoms and nearly 80 percent are not even aware of the infection. Source: http://www.khon2.com/news/local/story/Four-confirmed-dengue-fever-cases-12-more/JCiNdCQ360i-g75C55M7tg.cspx

Transportation

Trucking execs asked to be terror-aware. A tractor-trailer filled with hazardous materials could be terrorists' next weapon of mass destruction, according to a panel of terrorism experts gathered in Concord, North Carolina, April 6. And the group encouraged trucking executives to play the front line of defense in guarding against such an attack. A terrorism panel expert with the FBI said terrorism is changing. Future attacks are more likely to be conducted by one person, "a lone wolf," he said, such as the Fort Hood shooter, the Christmas underwear bomber, and the Times Square bomber. "We need your industry's help in identifying these lone offenders," he said. More than 100 trucking executives attended the 1-day security conference at Charlotte Motor Speedway that focused on improving ties between the government and industry leaders. The panel included experts from the FBI, DHS, and Transportation Security Administration. Some speakers referred to truck drivers as "American road warriors" and "road patriots." They urged the executives to conduct extensive background checks on their drivers and look for unusual changes in their lifestyles, and to be aware of materials being transported to or from odd locations. Source: http://www.charlotteobserver.com/2011/04/07/2203750/trucking-execs-asked-to-be-terror.html

Report finds thousands of U.S. bridges in dangerous need of repair. The week of March 28, a new report found that nearly 12 percent of the bridges in the United States were "structurally deficient" and required replacement. The report, prepared by Transportation for America (TOA), an advocacy organization made up of business, transportation, and environmental organizations, found that 69,000 bridges are in need of major repairs and critical maintenance has often been delayed as states are struggling with budget shortfalls. Pennsylvania is the state with the largest number of deteriorating bridges with more than one out of four bridges in need of repair – 5,906 out of a total of 22,271. Oklahoma, Iowa, Rhode Island, and South Dakota rounded out the top five states with the highest number of aging bridges. More than 20 percent of bridges in those states were structurally deficient. The average age of bridges across the country is nearing 42 years, and most were designed to have a 50 year lifespan before they were replaced or reconstructed. TOA has called for increased

funding for infrastructure to help make repairs. The report noted the American Society of Civil Engineers has recommended the United States spend $17 billion per year on bridge maintenance, significantly more than the $10.5 billion that is currently spent each year. Source: http://homelandsecuritynewswire.com/report-finds-thousands-us-bridges-dangerous-need-repair

FAA issues emergency order to inspect airliners. Federal officials have issued an emergency order requiring inspections of Boeing planes with similar construction to the Southwest Airlines plane that had a 5-foot tear that led to an emergency landing the week of March 28. The Federal Aviation Administration (FAA) order April 5 applies to Boeing 737-300s, 400s and 500s that have a similarly constructed joint where pieces of the plane's skin meet. The joint is at about the midpoint of the passenger cabin. Nearly all of the U.S.-registered planes covered in the order have already been re-inspected. FAA has previously said the order will affect 80 U.S. planes, 78 of which are operated by Southwest. The other two are operated by Alaska Airlines. Southwest has said it has finished their inspections, finding five more planes with similar signs of metal fatigue. Source: http://www.businessweek.com/ap/financialnews/D9MDNO8G1.htm

NTSB: Cracks similar to those found in damaged Southwest Airlines jet found in 3 other planes. Inspectors have found small, subsurface cracks in three more Southwest Airlines planes that are similar to those suspected of causing a jetliner to lose pressure and make a harrowing emergency landing in Arizona, a federal investigator said April 3. Southwest said in statement that two of its Boeing 737-300s had cracks and will be evaluated and repaired before they are returned to service. A National Transportation Safety Board (NTSB) member said April 3 that a third plane had been found with cracks developing. Checks on nearly 60 other jets are expected to be completed by April 5, the airline said. That means flight cancellations will likely continue until the planes are back in the air. About 600 flights in all were canceled over the weekend after Southwest grounded 79 of its planes. Nineteen other Boeing 737-300 planes inspected using a special test developed by the manufacturer showed no problems and will be returned to service. April 1's flight carrying 118 people rapidly lost cabin pressure after the plane's fuselage ruptured causing a 5-foot-long tear — just after takeoff from Phoenix. Oxygen masks were deployed and the pilots made a controlled descent from 34,400 feet into a southwestern Arizona military base. No one was seriously injured. The tear along a riveted —lap joint near the roof of the Boeing 737 above the midsection shows evidence of extensive cracking that had not been discovered during routine maintenance before the flight and probably would not have been unless mechanics specifically looked for it — officials said. An examination showed extensive pre-existing damage along the entire tear. The NTSB has not determined that the cracks caused the rupture, but it is focused on that area. Further inspection found more cracks in areas that had not torn open. Source: http://www.washingtonpost.com/business/ntsb-cracks-similar-to-those-found-in-damaged-southwest-airlines-jet-found-in-3-other-planes/2011/04/03/AFTBMRTC_story.html?hpid=z3

Water and Dams

(Arizona) **Waste water worker charged with terrorism.** A city of Mesa Water Resources employee was charged with terrorism and making terrorist threats after he turned off numerous waste water treatment operating systems at a facility in Gilbert, Arizona, in the early hours of April 1, police said. The Greenfield Water Reclamation Plant near Greenfield and Queen Creek Roads is a massive facility.

Fourteen buildings on the campus transform sewage from Gilbert, Mesa, and Queen Creek into water suitable for irrigation. Authorities said the 43-year-old employee was the sole treatment plant operator working the midnight shift. Armed with a handgun, he walked through the facility alone, methodically turning off major operating systems at the plant. He is certified through the Arizona Department of Environmental Quality as a waste water treatment operator. Left untreated, the sewage in the system would cause a buildup of methane gas, which could cause a huge explosion. City workers were emphatic that the public not be alarmed. They said nobody was harmed, and the safety mechanisms in the plant worked as expected. For an unknown reason, the suspect called 911 about 2:40 a.m. almost 3 hours after they say he had begun to sabotage the utility. SWAT officers negotiated with him for 2 hours before arrested him. Police said he had a gun on him when they took him into custody. During the 2-hour standoff, SWAT officers escorted waste water employees through the campus, restarting the major systems. The suspect had worked for Mesa's water resources department since 2007. Police have not released a possible motive. Source: http://www.kpho.com/valleynews/27403898/detail.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**